CLAIMS

What is claimed is:

1. An automated process of detecting security vulnerabilities present in a target Web site, comprising the steps of:

establishing an Internet connection with the target Web site;

retrieving a default Web page for the target Web site;

parsing through the default Web page to identify any linked-to Web pages which are referenced by the default Web page;

parsing through the default Web page to identify any hidden Uniform Resource Links (URLs);

scanning the target Web site to detect the presence of at least one exploit, and recording any detected exploits; and

outputting the security vulnerabilities, comprising the successful exploits.

2. The method of claim 1, further comprising applying at least one predetermined hack method to the linked-to Web pages and outputting a response from the target Web site to each hack method.

3. The method of claim 2, wherein the predetermined hack method comprises issuing a request to the target Web site wherein a file extension of a valid Web page is changed to determine whether an old version the valid Web page is available at the target Web site.

4. The method of claim 1, further comprising parsing through the linked-to Web pages to identify any further-linked-to Web pages which are referenced by the linked-to Web pages.

5. A system for detecting security vulnerabilities present in a target Web site, comprising:

a. memory for storing:

1. a valid Web page database;

2. a vulnerable Web page database;

3. at least one exploit; and

4. a security vulnerability database; and

b. a processor connected to the memory and being configured to establish an Internet connection with the target Web site, retrieve a default Web page for the target Web site, parse through the default Web page to identify any linked-to Web pages which are referenced by the default Web page, parse through the default Web page to identify any hidden Uniform Resource Links (URLs), scan the target Web site to detect the

presence of the at least one exploit, record any detected exploits, and output the security vulnerabilities comprising the successful exploits.